Computer Crime 7

The Internet is the new frontier for most professional investigators. Computers are not simply useful tools to make the job of an investigator easier; they are also a necessity for remaining in business. Those who do not operate on the World Wide Web will soon become as extinct as the dinosaur.

In the United States, all financial institutions report incidents of frauds committed against them to the Securities and Exchange Commission (SEC). The amount of computer fraud as a product of the increasing use of computers will grow unless computer security can eliminate traditional frauds by employees.

Computer Crimes

A computer crime is defined as an illegal act in which knowledge of computer technology is used to commit the offense. According to the Federal Bureau of Investigation (FBI), 21 states have enacted laws dealing with computer crime, but there is little consistency from state to state, and several have failed to deal with hackers who enter the systems for fun rather than profit. Computer manipulation crimes involve changing data to create records in a system for the specific advancement of another crime. Virtually all embezzlement in financial institutions requires creation of false accounts or modification of data in existing accounts. The perpetrator does not need to know computer programming but must have a good sense of how to operate the system.

The FBI categorizes computer crime into five groups, and not all involve financial transactions. Computer thieves can also steal goods and services, college degrees, and titles to properties, as well as negotiable securities. The five categories of computer crimes are system deceit/unauthorized transactions, system alteration, physical destruction, theft of information, and time theft—that is, unauthorized use of the computer.

It is estimated that 85% of computer fraud cases are never reported because of embarrassment, loss of public confidence, false arrest concerns, and overall difficulty of prosecution.

Institutions are heavily dependent on automated systems and electronic transfers of funds for various business activities. They are exposed to the possibility of significant fraud in the computer area, because computer records

are in electronic form, and computer processing of accounts and transaction data may be performed by a group of persons outside the financial institution. Additionally, transactions may be initiated from remote facilities by various employees, customers, and external parties.

The following are necessary to maintain the security of a computer system and electronic transactions:

- Adequate physical security to prevent accidental or intentional damage to the computer system and related equipment
- Software and data file security to ensure that computer programs and data files are not altered accidentally or deliberately
- Techniques for maintaining transaction data controls and for analyzing the reasonableness of transactions so as to detect and report possible crime attempts
- Use of customer identification methods to restrict unauthorized individuals from initiating transactions to customer accounts
- Secure communications networks to prevent unauthorized interception of or alteration of electronic data
- Adequate internal controls to prevent, detect, and correct computer crime and other concerns

Computer Fraud

Any incident involving computer technology in which there is a victim who suffered (or could have suffered) a loss and a perpetrator who intentionally made (or could have made) a gain is defined as computer fraud.

An indicator of possible problems is present in some, or all, of the following elements of a vulnerable computer system (five tip-offs of computer-related fraud):

- The computer generates negotiable instruments or is used to transfer credit, process loans, or obtain credit ratings.
- Employee relations are poor; dismissed data-processing personnel remain on the job until their termination dates; or a computer programmer is overqualified for the job, with the possible result that bottled-up creativity will seek undesirable outlets.
- Separation of key personnel is inadequate, in terms of either responsibility or physical access.
- After-hours data-processing operations are loosely supervised.
- Auditors have little expertise or background in computer operations.

Indicators that require follow-up investigation include situations in which the following occur:

- Computer reports or copies of pertinent forms are inside the trash bins.
- Auditors are not involved in the development of application programs, resulting in the absence of built-in checks and balances.
- The industry is depressed, yet computer-generated data indicate record sales for the company.
- Frequent violations are reported of the rule that requires that at least two people should be present when data-processing equipment is operated.
- Computer operations, including storage of output data, can be viewed by the general public.
- System components are near open windows, next to outside walls, or in front of open doors (easily accessible).
- The personnel department submits candidates for data-processing positions with only routine screening. The chief weakness of computer systems is people.
- Data preparation equipment is easily available and loosely controlled.
- Access to computer facilities is not limited to those with a need to be there.
- Transactions are rejected by the system, because they did not pass one or more control points or were put aside, ignored, or deliberately overridden.
- Increase is noted in employee complaints about overwithholding by the computer or about inaccuracies in the year-end earning statements.
- There is a surge in customer complaints about delays in crediting their accounts.
- Key forms, such as purchase orders, invoices, and checks, are not numbered sequentially.
- Continuous-form checks are not stored securely.
- The bill for use of computer time is much larger than the computer time logs seem to indicate it should be.
- Access to central processors is attempted from a remote terminal whose exclusive user is on vacation.
- Payments are sent to new suppliers, but they are not listed in company directories.

The Computer Crime Investigator

The computer crime investigator is a specialist in criminal investigation, data processing, auditing, and accounting. His or her knowledge of data

processing should include computer operations, systems design and analysis, programming, and project management.

A primary element in a computer crime investigation course is the manner in which it is structured and whether it contains all the vital areas of required knowledge. A computer crime investigation curriculum should include the following:

- The types of threats and vulnerabilities to which a computer is susceptible
- Data-processing concepts relative to software (programming) and hardware (the equipment)

Investigative Methodology

Investigative methodology includes investigative procedures, forensic techniques, review of technical data systems, investigation planning, interview and interrogation techniques, information gathering and analysis, and case presentation techniques.

The Investigative Process

Most computer frauds are complex, hidden, and extensive. The detection of wrongdoing is usually first noticed by the internal auditor. The investigator must then establish essential elements of the crime to support successful prosecution; identify, gather, and protect evidence; identify and move closer to suspects; identify patterns of action and behavior; determine probable motives, which will often identify potential suspects; provide accurate and objective facts upon which judgments concerning discipline, termination, or prosecution may be based; and identify weaknesses in control and counter them by revising existing procedures or recommending new ones, and by applying security equipment, where justified.

The first step in the investigation of computer fraud is to establish that a loss of asset occurred; the process should determine that an asset was accountable for at some point and definitely missing at another point. The second step is to establish the facts. Get as much information as possible from everyone involved. Interview anyone who may have had control or access to the asset during the established time frame. Finally, gather evidence, organize data, examine documents for forgeries, and look for "out of balance" conditions.

Areas of Computer Abuse

The following are the most likely areas where computer abuse will occur.

Payroll

Fictitious personnel can be created.

Inventory

Fictitious accounts can be created and records falsified to show bills were paid, while inventory was delivered to fictitious persons and locations.

Accounts Receivable

This information can be mismanaged by a loss of computer records of monies owed to the firm.

Disbursements

Through manipulation of data, a company may be tricked into paying for goods and services that were never received.

Operations Information

This data can be very valuable to a firm's competitors, especially in the areas of growth plans and new designs.

Telecommunication Crimes

Telecommunication crimes involve illegal access to or use of computer systems over telephone lines. A hacking program tries to find valid access codes for a computer system by continually calling the system with randomly generated codes. Use of a hacking program constitutes unauthorized access to a system, and access codes generated by a hacking program are stolen property. Misuse of telephone systems also falls into the telecommunications crime group. *Phone phreaking* and *BBSing* are terms used to describe telephone frauds in which stolen or false telephone access cards are used to pay for long distance telephone calls.

Computer Manipulation Crimes

These types of crimes involve changing data or creating records in a system for the specific advancement of another crime, usually theft. Virtually all embezzlements in financial institutions require the creation of false accounts or modification of data in existing accounts to perform the act.

Hardware and Software Thefts

These thefts characterize the illegal use of a computer. Software piracy involves the duplication of programs without authorization or payment. Virtually millions of dollars are lost by software developers to this type of crime each year, even though vendors are now attempting to safeguard their programs through the use of copyright protection devices.

Computer Losses

In an American Bar Association survey of 283 large companies, 48% admitted they had suffered from computer crime; 72 of them assessed their losses at between $145 and $730 million. The U.S. Chamber of Commerce estimates that computer crime losses total around $100 million per year; other estimates are closer to $500 million per year. The average computer crime loss is $500,000.

Methods of Attack

There are many ways to compromise a computer. Some are complicated technical attacks, while others can be accomplished with only a basic understanding of computer operations. The following are the most common methods of attack.

Data Diddling

This is the simplest, safest, and most common method used by insiders. It involves putting false information into the computer. The data are changed before or during input from a computer, such as fraudulent payroll information.

Trojan Horse

The computer criminal can alter the computer circuitry or a computer program by adding instructions unknown to the owner. As a result, the computer performs unauthorized functions (e.g., it deletes accounts payable or receivable).

Salami Slicing Techniques

Typically, this involves a money crime. It is an automated form of stealing small amounts of assets from a large number of sources.

Trap Doors

In the development of large application programs and computer operating systems, programmers often develop debugging aids that provide breaks in a code. These programs are made deliberately to change or alter existing

programs legitimately. These programs, called trap doors, provide computer abusers with the ability to alter data without detection.

Logic Bombs

These are illegal instructions that operate at a specific time or periodically after being given to a computer. They are often dependent upon date, time, or another operation for execution.

Trashing (Dumpster Diving)

This practice, also known as scavenging, is the surreptitious obtainment of information from discarded printouts, manuals, tapes, and disks. It often involves searching through trash bins for discarded computer listings or carbon sheets from multi-copy forms.

Piggybacking and Impersonation

Physical piggybacking is a method for gaining access to controlled access areas through the use of stolen or fraudulent cards. Electronic piggybacking involves gaining access to secured data through the use of someone else's password or identification sign-on. Compromise of the security system takes place when the computer verifies the sign-on but not the person. Impersonation is simply the process of one person assuming the identity of another, either physically or electronically.

Although most of the attention regarding the misuse of computers is given to criminal aspects of computer abuses, it is likely that civil actions will have an equally important effect on long-term security problems. The issue of computer crimes draws attention to the civil and liability issues in computing environments. In the future, there may be more individual and class action suits against businesses and employers. All of these give rise to a bright future for the investigator who specializes in computer-related investigations. This area is the fastest-growing area of need for the investigative industry. Not only is there a need for detection of events that occurred on the computer; there is also a need for an analysis of computer operations to safeguard the business community from outside abuse, misuse, and hacking. Systems security is now a need in all business communities that conduct business through a computer.

Institutional Vulnerability

Institutions are heavily dependent on automated systems and electronic transfers of funds for various business activities. They are exposed to the possibility of significant fraud in the computer area because of the following:

- Computer records are in electronic form.
- Transactions may be initiated from remote facilities by various employees, customers, and external parties.
- Computer processing of accounts and transaction data may be performed by a group of persons outside the financial institution.

Design and Personnel Rules for Security

Certain commonsense steps can greatly reduce the possibility of computer crimes:

- Locate the computer operations facility so that it cannot be viewed by the general public.
- Ensure that computer system components are not easily accessible and are not located next to outside walls, in front of open doors, or near windows.
- Use key forms with the system, such as purchase orders, invoices, and checks, and make sure they are always numbered sequentially.
- Have auditors present when application programs are developed so that checks and balances are automatically built into the design.
- Ensure that continuous-form checks are securely stored.
- Establish strong rules about who is allowed access to computer facilities.
- Establish strong controls about data preparation equipment, and establish from the start who will have access to it.
- Provide for extensive background screening of individuals who will do data processing.
- Require that at least two persons be present when data-processing equipment is operated.
- Ensure that access to central processors is denied when exclusive users of remote terminals are on sick leave or vacation.
- Ensure that computer reports or carbon copies of pertinent forms are shredded or otherwise destroyed with a witness present.

Computer System and Electronic Transactions Security

Maintaining the security of a computer system and electronic transactions involves the following:

1. Adequate physical security to prevent accidental or intentional damage to the computer system and related equipment
2. Security of software and data files to ensure that computer programs and data files are not altered, accidentally or deliberately

3. Established techniques for maintaining transaction data controls and for analyzing the reasonableness of transactions to detect and report possible crime attempts
4. Use of customer identification methods (passwords, encryption, etc.) to restrict unauthorized individuals from initiating transactions to customer accounts
5. Maintenance of a secure communications network to prevent unauthorized interception or alteration of electronic data
6. Insurance of adequate internal controls to prevent, detect, and correct computer crime and other concerns

Tip-Offs to Possible Computer Fraud

An indicator of possible problems is present in some, or all, of the following elements of a vulnerable computer system (five tip-offs of computer-related fraud):

- The computer generates negotiable instruments or is used to transfer credit, process loans, or obtain credit ratings.
- Employee relations are poor; dismissed data-processing personnel remain on the job until their termination date; or a computer programmer is overqualified for the job, with the possible result that bottled-up creativity will seek undesirable outlets.
- Separation of key personnel is inadequate, in terms of either responsibility or physical access.
- After-hours data processing operations are loosely supervised.
- Auditors have little expertise or background in computer operations.

Areas of Computer Abuse

- Payroll—Fictitious personnel can be created.
- Inventory—Fictitious accounts can be created. Records can be falsified to show that bills were paid, while inventory was delivered to fictitious persons and locations.
- Accounts receivable—There can be a loss of computer records of monies owed to the firm.
- Disbursements—Through manipulation of data, a company may be tricked into paying for goods and services never received.
- Operations information—This data can be very valuable to a firm's competitors, especially in the areas of growth plans and new designs.

Guidelines for Conducting an Investigation (Insider Suspect)

1. Opportunities:
   a. Familiarity with operations
   b. Position of trust
   c. Close association with suppliers and other key people
2. Situational pressures—financial:
   a. High personal debt
   b. Severe illness in family
   c. Inadequate income or living beyond means
   d. Extensive stock market manipulation
   e. Loan shark involvement
   f. Excessive gambling
   g. Excessive use of alcohol or drugs
   h. Heavy expenses incurred from extramarital involvement
   i. Undue family, peer, company, or community expectations
3. Situational pressures—revenge:
   a. Perceived inequities (e.g., low pay or poor job assignments)
   b. Resentment of superiors
   c. Frustration, usually with the job
4. Undesirable personality traits:
   a. Low self-esteem
   b. Lack of personal honesty
   c. No well-defined code of personal ethics
   d. A wheeler-dealer (i.e., someone who gives feelings of power, influence, social status, and excitement associated with rapid financial transactions involving large sums of money)
   e. Arrogant or egocentric
   f. Neurotic, manic depressive, or emotionally unstable
   g. Psychopathic
   h. Personally challenged to subvert a system of controls

Conduct Thorough Background Investigations

In addition to evaluating suspects in terms of opportunities and situational pressures (financial or personal), the investigator should construct a personal biography on all known suspects. The biography should include the following:

1. Criminal history
2. Review of personnel file for such things as a record of excessive absences, counseling, reprimands, and other disciplinary actions
3. List of associates

4. References (if not verified, do so during the investigation)
5. Documented comments from former employers

Appendix 7.1: Investigation of Computer Fraud

When investigating what appears to be an inside computer crime, the factors listed previously, in "Guidelines for Conducting an Investigation (Insider Suspect)" should be taken into account.

Investigators should also construct a personal biography of suspects composed of three factors: criminal history, list of associates, and references.

Appendix 7.2: Computer Crime

Profiling the Computer Criminal

Profiles on computer criminals should include the following:

- Tools or devices used
- Computer or other skills demonstrated in the crime
- Orientation as to politics, religion, or interest in pop culture, which forms a subtext of the crime (i.e., reference to religion, gangs, political movement, etc.)
- Files may provide a clue as to information a suspect is looking at and how that information would be used (Who would benefit from having that information?)
- Evidence as to the criminal's personality and way of thinking (Is suspect well organized or impulsive? Was the crime planned in advance with meticulous detail or was it a random, haphazard event?)
- Occurrence of crimes in any logical pattern (day, date, time of day) or random times and days
- Unusual qualities in the method of attack on software or hardware or the altering of information on the computer

Investigative Procedures on Malicious E-Mail

- Preserve the evidence.
- Trace the e-mail's path through your system with the help of the network administrator. Be on the lookout for any bypasses of e-mail security.
- Obtain complete e-mail records of individuals involved for the preceding 30 days.
- Review all personnel files.

- Interview the individuals involved. Get their version on the record. Who had access to their computers? Why?
- Interview coworkers, witnesses, supervisors, and so on.
- Follow the audit trail.
- Inspect the computers involved for signs of tampering, unauthorized access, and so on.
- Compare stories, events, and evidence against all other records, access logs, terminal logs, and so on.

Indications of Suspicious Behavior by Employees

- People who never take a vacation
- Workers with excessive overtime, living at the job, and who are always around the job site
- Employees with a criminal record, history of substance abuse, or gambling problems
- Employees with constant financial problems
- Workers with extreme political views or radical lifestyles

Examine the elements of the crime, and analyze what is necessary to commit the crime, such as knowledge of software used, knowledge of how to create a logic bomb—an accomplice in accounts payable, a mail drop to receive the checks, dummy businesses to act as vendors, fake IDs to open bank accounts, and bank accounts to negotiate the checks.

Analysis of these elements gives the investigator new avenues to explore and leads to follow (e.g., an accomplice within the company). Physical evidence of penetration of computer security includes broken glass, cut wire fences, picked locks, cut locks, jimmied doors, disabled security cameras, changed locks, security guards unable to access the computer area, holes cut in walls or doors, and disabled alarm systems.

In cases of embezzlement, you need to analyze the flow of data and documents through the financial processing system (FPS). Determine the following:

- What steps are required to issue a check?
- Where are the checks printed? Who has access to that area?
- What steps are necessary to have someone added to the payroll?
- Is it possible to change information within the FPS programs? How?
- Is there an FPS paper or audit trail? How does it work?

Conducting Internal Investigations

The Risk Matrix

The risk matrix includes opportunity factors as well as means, motive, and high risk factors. Included in opportunity factors are events that occurred on the suspect's shift, or just before or after; whether the suspect is knowledgeable about the work involved; whether the suspect had the necessary skills to commit the event; whether there is a relationship between the suspect's actions and the event; and whether the suspect has an alibi.

Included in the means factors are whether or not the suspect had access to the area, whether or not the suspect possessed access materials to the area, and whether or not the suspect had the ability to bypass security to obtain access to the area. Motive factors include the suspect having high risk factors, the suspect having resentment against the company, and the suspect having political grievances. High risk factors include family problems, financial problems, a lifestyle beyond salary means, coworkers suspicious of the suspect, the suspect acting defensive during interviews, substance abuse or gambling problems, and other suspicious lifestyle factors (extramarital affair, cult activity, etc.). Anyone who exhibits characteristics within the risk matrix should undergo the following investigation:

- Review personnel records.
- Interview previous coworkers and supervisors.
- Review the suspect's work product.
- Conduct an extensive background check of the suspect.
- Interview current associates.
- Make asset searches.
- Provide surveillance of the suspect after work.
- Interrogate the suspect once incriminating evidence is found.

Conducting External Investigations

The investigator should cooperate with police or any other investigative agency; preserve evidence and the crime scene; obtain the dollar loss and provide documentation; obtain intelligence information; identify and interview witnesses and suspects; and question vendors, suppliers, and visitors.

Report Writing

Your report should include a summary of the incident, a description of the evidence establishing a *corpus delicti* (body of the crime), a description of how the crime was committed and the suspect's motive, the financial impact of the crime, and a review of the evidence identifying those responsible.

If the crime was committed by an employee of the company, your report should provide the employee's history with the company, any previous disciplinary problems, criminal history, family background, amount of gain from the crime, and the suspect's financial resources.

If the crime involved a vendor, supplier, or contract worker, your report should provide a history of the relationship with the company, the compensation received, background on the suspect, criminal history, profit from the crime, and the insurance coverage and financial stability of the employer.

If the crime was committed by another company, your report should provide a background of the other company and its officers, a criminal background check of the officers, profit from the crime, and the applicable insurance.

If the crime was committed as part of an ongoing criminal enterprise (Racketeer Influenced and Corrupt Organizations [RICO] Act), your report should provide a pattern of criminal activity, the types of crimes involved in the pattern, and the evidence proving the crimes.

Appendix 7.3: The Internet and the World Wide Web

The Internet is a worldwide network of computers that allows a multitude of types of computers to communicate with each other. Information may be sent or received. The Web is part of the Internet and may be accessed to use text, graphics, sounds, and animation; for commercialization purposes, there are unlimited "pages" or Web sites, and the Web provides hypertext on links.

E-mail is noted for its ease of use, speed, and its multiple addressing capability. It is an inexpensive method of communication.

Search engines are convenient methods of finding information; they are home page locators that provide various searching methods when you register with the search engines. There are over 40,000 newsgroups. One well-known newsgroup is Usenet, also called net news. E-mail messages may be posted to newsgroups such as Alt.private.investigator.

The Universal Resource Locator (URL) provides information page addresses. Users need only to type in an address or click to link. This is the most common hypertext transfer protocol that directs users to home pages.

There are numerous search tools with broad-based search engines containing subject directories, meta search engines, and specialized search tools. The top search engines include Google, Yahoo, Hotbot, AltaVista, Excite, e-infoseek, Lycos, and WebCrawler. There are also subject directory engines like Yahoo and Virtual Reference Desk.

To structure a search, review search engine techniques. Read the FAQ section of the search engine, and focus the search using primary and secondary words.

Meta search engines are useful for searching several engines at the same time. Remember to keep search terms simple. Metacrawler, dogpile, and Inference Find may also be used.

If you cannot find the results you are seeking, reconsider search terminology, check the spelling and truncation, use specialized search engines, post your inquiry to discussion groups or listserves, and contact your local librarian.

For professional investigators who work in the corporate world, I highly recommend that you obtain a copy of *The Art of Deception: Controlling the Human Element of Security*, by Kevin D. Mitnick, William L. Simon, and Steve Wozniak (Wiley, New York, 2003). Mitnick is the legendary hacker who was sent to federal prison for his exploits. Released in 2000, he is now a security consultant to Fortune 500 companies that wish to avoid hackers getting into their computer systems. Chapter 16 in his book is entitled "Recommended Corporate Information Security Policies." He states that if these policies were in effect, he would not have been able to hack into the systems he did. This should be considered the bible for those wishing to avoid cyber desperadoes.

Computer Forensics

The Online Security Primer for Recovering Electronic Digital Evidence

How Hard Drives Work

A hard drive (such as the "C" drive) contains hard round flat disks (known as platters) coated on both sides with a magnetic material designed to store information as binary numbers (magnetic patterns of 0's and 1's). The platters are mounted on a spindle that rotates at high speed, generally 5,000 to 10,000 rpm.

Electromagnetic read/write devices, known as "heads," mounted on sliders and connected to an actuator arm, are positioned over the surface of the disk. A logic board controls the motion of the heads, the process for reading and writing data, and the protocol for communicating with the rest of the computer.

Conceptually, the inside of a hard drive is similar to the inside of an old jukebox, with the record being the platter, the jukebox tone arm being the hard drive's actuator arm, and the needle being the read/write heads.

How Data Is Stored

The surface of each platter can hold tens of billions of individual bits of data. Groups of bits, of either a 0 or 1, could be eight, sixteen, or thirty-two bits in length. These bits form a "byte," representing an alphabetical character or numerical number. Most desktop and server hard drives are 3.5 inches in diameter and notebook PCs have 2.5-inch and 1.8-inch drives. A large

capacity drive, measured in gigabytes (GB), can store hundreds of billions of individual bits of data and is commonly available for under $200.

Each platter has two surfaces capable of holding data (the top and bottom), and each surface has a read/write head. Thus on a hard drive with three platters, there are a total of six "surfaces" with information being read by six heads.

The recording surface of each platter is divided into concentric tracks (circles), and the vertical area of similar tracks on multiple platters is referred to as a "cylinder." These tracks are further subdivided into sectors and clusters, which are groups of sectors. The logical organization of information on the platter is similar to slices of a pie. Data is stored in all sectors of each track, except parts of the outside track, which is generally reserved for the file allocation table (FAT) directory. The FAT contains the file names and the locations of active files on the disk. The file allocation table tells the computer's operating system which sectors (the "geographic location") contain data. A sector typically will hold 512 bytes of data (about the length of this sentence), plus "address" information used by the drive controller circuitry. There can be over 40 million sectors on a 20-GB hard drive. "Formatting" a hard drive is the process by which the disk surface is organized into tracks and sectors.

Sectors are also grouped sequentially into clusters, and generally there are 32 sectors per cluster. More often than not, data is stored sequentially in sectors within the clusters.

Reading and Writing Digital Data

When a user clicks on a file to open it, the application being used passes the file name to the computer operating system, which consults the FAT to determine the address (platter track and sector) where the first portion of the file is located. The operating system transmits this information to the disk controller, which positions the heads on the actuator arm over the correct physical location. The initial cluster will contain the address of subsequent sectors from which the controller must retrieve data. The controller retrieves the packets of data and reassembles them in the correct order before sending the "file" to the central processing unit (CPU) for display on the screen.

Disk systems, unlike tape, do not store records together physically. With tape, each time a change is made to a block of data, such as an insertion in a text file, the entire block of "data" is rewritten onto the tape with the new data incorporated. When a similar change is made to text stored on disk, the **original** file usually remains intact. The disk controller checks the file allocation table for the location of an unallocated cluster (a group of sectors available to store data), and inserts the data there.

Thus the various parts of a file, such as this article, can be scattered randomly among hundreds of sectors and clusters on various tracks. [Hence the term, random access device, meaning a drive that can retrieve or store data

in any order to any location on the disk. Sequential access devices, such as backup tapes, store data in sequential order, and are unable to retrieve data as quickly.]

Allocated clusters contain data that is "active" according to the file allocation table.

Unallocated clusters may contain data, but in storage space that the computer is no longer using for active files (see Deleted Files below). Thus, although unallocated clusters frequently contain "residual" data, this space will be randomly used (overwritten) to store new active data.

Why Is Deleted Not Always Deleted?

When a user deletes a file, the operating system only deletes the first letter of the file name from the file allocation table, and reports the sectors containing the "deleted" data as "empty," or available for the storage of new data. However the old data remains unchanged and "intact" until new data is stored in the specific sector and cluster containing the "residual" data. It is during this process of "overwriting" new data into the sectors containing the old data that the residual data is truly deleted. However, since data is randomly stored into the millions of potentially available sectors, it is unusual for all sectors containing a file to be overwritten with new data. This provides the opportunity for portions of deleted files to be recovered from "unallocated" clusters long after the user has deleted the file from the computer.

The Process for Recovering Electronic Evidence

There are two primary steps for recovering electronic data. The first is the "acquisition" of the target media, and the second is a forensic byte-by-byte analysis of the data. Utilizing special computer forensic tools, the target media is acquired through a noninvasive procedure by making a complete sector-by-sector bit-stream mirror image.

During the imaging process, it is critical that the mirror image of the target drive be acquired in a DOS environment. Turning on the computer and booting into the operating system (usually Windows) will subtly modify the file system and destroy some potentially recoverable evidence.

The resulting image becomes the "evidence file," which is mounted as a read-only or "virtual" file, on which the forensic examiner will perform an analysis of the data. The forensics software used by Online Security will create an evidence file that will be continually verified by a Cyclical Redundancy Checksum ("CRC") algorithm for every 64 sectors (block) of data and by a MD5 128 bit encryption hash file for the entire image. Both steps verify the integrity of the evidence file, and confirm the image remains unaltered and forensically intact, and that critical date and time stamps remain unchanged. (Under MD5 hash encryption, changing one bit of one byte of data will result

in a notice stating that the evidence file data has been changed and that the evidence is no longer forensically intact.)

Searching Digital Evidence

Specialized forensic software provides several methodologies for searching the evidence file. Multiple pieces of evidence, for example two hard drives, a floppy and a multiple session CD-ROM, can be searched, sorted, and analyzed simultaneously.

A Windows Explorer view displays the files and folders of the target hard drive in an easy to browse format. Each file is displayed in a spreadsheet format where the files can be sorted and filtered under numerous fields. The examiner can designate which files to include in this view, such as files from a single folder or a single volume. A preview pane displays the highlighted files allowing the examiner to easily scroll through individual files. A hex/text viewer shows the contents of any file, with the file slack—portions of unallocated clusters—shown in red. Search hits are highlighted automatically.

Forensic search utilities are used to search for keywords in order to locate relevant documents. These searches will locate any "bytes" of data matching the search term.

The development of effective search terms is a critical component of recovering digital evidence and will be a major factor in the success of the forensic investigation. As an example, searching for the word "info" may locate tens of thousands of hits where the letters "info" were used in a file or line of code. Redefining the search for "info@OnlineSecurity.com" will help narrow the number of responses. Reviewing the hits from the word keyword searches consumes a major portion of the time resources necessary for searching digital evidence. Narrowing the search to terms or phrases that are unique to the specific case situation will enhance the results and reduce the cost.

Forensic software will also locate drafts of documents, back-up files (.bak, .wbk), temporary files (.tmp), cache files, autosaves, registry data, and residual data. Advance searches can be conducted for "general formats" such as telephone numbers, network ID, logon records, or Internet protocol addresses (IP numbers), even when the specific number is not known.

Time and date stamps, access logs, and recycle bin activity are often a critical focus of the investigation and can be recovered. Files (but not residual data) can be sorted by creation date, last accessed, or last saved. Swap files and file slack, which are locations on the disk where deleted residual data often resides, can be recovered. Print spooler files, with their original time stamps, can be recovered and reviewed. Files that were recently accessed can be determined and a list of all Internet sites (URL's) accessed, and the time and date of access, can be compiled. Also, a forensic picture gallery

automatically identifies all graphic files and displays them as thumbnails that can easily be copied onto a CD-ROM or thumb drive.

Forensic investigators will also be able to identify any attempts to hide a file by merely changing its name. Each file's extension (i.e., .jpg, .gif, .doc) is matched against the file's actual "signature" to determine if an attempt has been made to "hide" the file. If a file was created in Word (.doc) and the extension was changed to .jpg, the forensic examiner is able to identify and flag that file.

Advantages of Digital Evidence

In addition to the advantages of recovering deleted files, digital evidence contains a wealth of critical data and "embedded" information for both intact files as well as deleted files. For example, forensic software can view the contents of a PowerPoint file to reveal (depending on how it was configured by the user) information such as: the creation date and original author; dates the file was last accessed, modified, and printed; when the file was last saved and by whom; the number of times the file was edited, for how long, and by whom; the number of revisions; client name, id and matter number; hidden key words and comments that identify who edited or collaborated on the file; and the original file location.

WordPerfect allows the user to open a saved file and "undo" the last 20 or so entries, charting the latest changes that have been made to the document. Word has a tracking device that can be secured with a password that can invisibly track **ALL** changes made on a document allowing a subsequent user with a password to review every keystroke and peruse every comment made to the document.

Searches also could reveal embedded information in e-mail headers including routing details and a list of associated file attachments. Palms and other digital assistants leave a log of when they were last synched with the desktop, and what information was downloaded. WinFax keeps a log file of all electronic faxes sent, sometimes for years after the original document was lost or destroyed.

Effective Strategies for Electronic Discovery

Prior to conducting on-site electronic discovery, preliminary information pertaining to the target machine and operating systems must be determined. Each computer system (platform) is different, and poses different types of technological issues for the effective and non-invasive imaging of the drive. Determining in advance whether the computer is a desktop or notebook, the size and type of the hard drive, the manufacturer and year of manufacture, the operating system, and the type of browser and e-mail package being used (Netscape mail, Outlook, AOL, etc.) is critical and will eliminate the potential for numerous technological glitches in the field. Each computer may

require a different type of interface and adaptor. Additionally, determining the system architecture of the opponents' premises will assist the forensic investigative team in verifying that all applicable systems and source media are identified and imaged.

In addition to the "traditional" locations of electronic evidence, such as computer hard drives, off-site servers, mirror sites, backup tapes, and removable media such as diskettes, etc., critical evidence may exist in a number of other locations. Some fax machines contain exact duplicates of the last several hundred pages of documents transmitted and received. Digital telephone systems may contain computer logs of all calls made and received, and often store voice mail messages in digital form on hard drives (.wav files).

Network audit programs (if properly configured) can contain a history of all files accessed, downloaded, or printed. Network firewalls monitor all web sites visited, external (outside of the Network) communication and information transmitted or received from the Internet.

Steps to Preserve (or Destroy) Electronic Evidence

Preservation of electronic evidence is critical. Depending on numerous factors, electronic evidence can be very perishable, or can last for years. The key to the success of electronic discovery and forensic investigations is to gain access to (or preserve the integrity of) the target media as quickly as possible. Relevant target media includes not only PC hard drives, but other types of storage media including tape backups and archives, floppy diskettes, PDAs (personal digital assistants such as Palms), and other removable electronic media.

Recently we have observed an increase in the types of actions that can impact the integrity and availability of electronic evidence including: (1) the use of data compression, disk de-fragmentation, and optimization programs; (2) the downloading or transfer of large files (such as .jpg pictures) which rapidly overwrite data in unused clusters; (3) the use of programs that overwrite sectors with a string of 0's, such as Norton Utilities' Wipe-Info; (4) the reuse of back-up tapes; (5) installing new software applications; (6), low level formats, operating system formats, partitioning formats, etc.; (7) deleting of temporary Internet files, browser history, and cookies; and (8) changing of the time clock on the computer. All of the steps taken above will destroy potentially recoverable evidence, and a number of the steps above could wipe the drive clean. Any of the steps above could alter, delete, or modify recoverable evidence.

Summary

During the last several years, there have been exponential advances in technology and with the advent of the Internet computers have become pervasive in everyday life. As a result, digital data in some form or another will be critical to most types of civil litigation and criminal proceedings.

The tools for conducting forensic investigations have also rapidly evolved, expediting the ability for securing evidentiary images, guaranteeing the integrity of digital evidence, and reducing the time and resources necessary for conducting a comprehensive investigation of electronic media.

There is a rapidly emerging trend to use computer forensics for a broad range of civil litigation matters involving intellectual property rights, trademark infringement, misuse and theft of trade secrets, patent and copyright violations, as well as more traditional matters such as employment law litigation and criminal fraud.